IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ROBERT WRIGHT, JOHNNY KULA, *Plaintiffs*, on behalf of themselves and similarly situated others, v. MASSACHUSETTS DEPARTMENT OF PUBLIC HEALTH, a Massachusetts agency, And MARGRET R. COOKE, Commissioner of the Massachusetts Department of Public Health, in her official capacity, *Defendants*.	CASE NO: _____ COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF JURY TRIAL DEMANDED

COMPLAINT

INTRODUCTORY STATEMENT

Conspiring with a private company to hijack residents' smartphones without the owners' knowledge or consent is not a tool that the Massachusetts Department of Public Health ("DPH") may lawfully employ in its efforts to combat COVID-19. Such brazen disregard for civil liberties violates both the United States and Massachusetts Constitutions, and it must stop now.

DPH developed a COVID-19 contact-tracing software application ("Contact Tracing App" or "App") for Android mobile devices (*e.g.*, smartphones and tablets) using an Application Programming Interface ("API") provided by Google, Inc. ("Google"). An initial version of the

App was made available in April 2021, but few Massachusetts residents voluntarily installed that version. To increase adoption, starting on June 15, 2021, DPH worked with Google to secretly install the Contact Tracing App onto over one million Android mobile devices located in Massachusetts without the device owners' knowledge or permission. When some Android device owners discovered and subsequently deleted the App, DPH would re-install it on to their devices. The App causes an Android mobile device to constantly connect and exchange information with other nearby devices via Bluetooth and creates a record of such other connections. If a user opts in and reports being infected with COVID-19, an exposure notification is sent to other individuals on the infected user's connection record.

Even if a user does not opt into the notification system, DPH's Contact Tracing App still causes the mobile device to broadcast and receive Bluetooth signals. This results in nearby devices exchanging Rolling Proximity Identifiers ("RPI"), which are randomly generated by the App and can be traced to each device owner with a "Key" generated by the App and held by DPH. The exchange of data also includes device identifiers known as media access control addresses ("MAC addresses"), which can be associated with specific device owners or locations. The exchanged data, both random and non-random, are time-stamped and stored in each device alongside other personal identifiers, including the device owner's MAC address, wireless network IP addresses, phone numbers, and personal emails. When this stored data is written onto mobile devices' system logs, it becomes available to DPH, Google, application developers, device manufacturers, network providers, and other third parties with access to the logs. DPH and third parties can use the MAC address of a device owner and other personal identifiers to trace the logged data back to determine the individual identity of the owners. Those with access to the system logs can also use time-stamped data regarding MAC addresses of other devices and locations with which the device

connected to determine the owner's past contacts, locations, and movement. In sum, DPH installed spyware[1] that deliberately tracks and records movement and personal contacts onto over a million mobile devices without their owners' permission and awareness. On knowledge and belief, that spyware still exists on the overwhelming majority of the devices on which it was installed.

At least two dozen other States have developed COVID-19 contact-tracing apps using Google API. These other States engaged in community outreach and encouraged their residents to voluntarily download the apps and opt-in for contact tracing. Massachusetts, however, is the only State to surreptitiously embed the Contact Tracing App on mobile devices that DPH locates within its borders, without obtaining the owners' knowledge or consent. These secret installations not only invade owners' reasonable expectation of privacy, but they also intrude upon owners' property right in their mobile devices by occupying valuable storage space. Because the Massachusetts and United States Constitutions prohibit governmental entities from unreasonable searches and uncompensated takings, this Court should enjoin DPH's unconstitutional scheme.

Plaintiffs are individuals who own and use Android mobile devices and live or work in Massachusetts. DPH installed its Contact Tracing App onto each of Plaintiffs' Android devices without their awareness or permission, which amounts to a computer crime under federal and Massachusetts law. *See* 18 U.S.C. § 1030(a)(2); Mass. Gen. Laws Ann. ch. 266, § 120F. No statutory authority supports DPH's conduct, which serves no articulable public health purpose, especially since Massachusetts has ended its statewide contact-tracing program. Plaintiffs bring this action on behalf of a class of over one million similarly situated individuals challenging DPH's

[1] "The term 'spyware' generally refers to any software that is downloaded onto a computer without the owner's or user's knowledge. Spyware may collect information about a computer user's activities and transmit that information to someone else." Cong. Rsch. Serv., RL32706, Spyware: Background and Policy issues for Congress (Jan. 12, 2011), available at https://www.everycrsreport.com/reports/RL32706.html (last visited Nov. 8, 2022).

clandestine and *ultra vires* installation of spyware onto their personal mobile devices, violating their constitutional and common-law rights to privacy and property. Pursuant to 42 U.S.C. § 1983 and other statutes, they bring this action seeking injunctive and declaratory relief, as well as nominal damages.

PARTIES

1. Plaintiff Robert Wright, PhD, is a Senior Faculty Fellow at the American Institute of Economic Research ("AIER"), located in Great Barrington, Massachusetts. He splits his time between Great Barrington and his vacation home in New Jersey. DPH's Contract Tracing App was downloaded onto Professor's Wright's Android device on or around July 1, 2021, without his permission or awareness. Mr. Wright has since deleted the App from his Android device.

2. Plaintiff Johnny Kula is a resident of Windham, New Hampshire but is employed in Massachusetts. He travels to Massachusetts daily for work and personal reasons. Mr. Kula owns an Android device. DPH's Contract Tracing App was downloaded onto Mr. Kula's Android device on or around July 1, 2021, without his permission or awareness. Mr. Kula uninstalled the App after discovering it. However, on or around November 2021, Mr. Kula discovered the Contract Tracing App had again been downloaded onto his Android device without his permission or awareness.

3. The Department of Public Health is a governmental agency of the Commonwealth of Massachusetts with various responsibilities related to public health within that state. *See* Mass. Gen. Laws Ann. ch. 17.

4. Margret R. Cooke is named Defendant in her official capacity as Commissioner of the Massachusetts Department of Public Health.

JURISDICTION AND VENUE

5. This Court has federal-question and supplemental jurisdiction pursuant to 28 U.S.C. § 1331 and 28 U.S.C. § 1367 because the federal-law claims arise under the Constitution and statutes of the United States.

6. Venue for this action properly lies in this district pursuant to 28 U.S.C. § 1391 because all Defendants reside in Massachusetts and a substantial part of the events, actions, or omissions giving rise to the claim occurred in this judicial district.

7. This Court may issue a declaratory judgment and grant permanent injunctive relief pursuant to 28 U.S.C. §§ 2201-2202.

FACTUAL ALLEGATIONS

I. MASSACHUSETTS AND OTHER STATES LAUNCHED AND ENDED COVID-19 CONTRACT-TRACING PROGRAMS AFTER SUCH PROGRAMS PROVED TO BE INEFFECTIVE

8. In December 2019, a new coronavirus, known as SARS-CoV-2 appeared in China. SARS-CoV-2 causes an infectious disease known as COVID-19, which spread quickly across the world in 2020. The World Health Organization ("WHO") declared COVID-19 a global health emergency on January 20, 2020.

9. One tool that public health authorities have tried to use to control the spread of COVID-19 is contact tracing. This method of disease mitigation involves identifying individuals

who had contact with infected persons and notifying them of potential exposure so that they may be tested and isolated, if appropriate.

10. Contact tracing was widely used and believed to be effective during the initial stage of the pandemic. In April 2020, Massachusetts' DPH launched a contact-tracing program to identify and isolate residents who were infected with COVID-19.

11. By 2021, however, evidence indicated that "[c]ontact tracing was largely ineffective in slowing COVID-19 virus transmission and improving public health."[2] The perceived efficacy of contract tracing was further undermined by the availability of vaccines and new, highly infectious COVID-19 variants.[3]

12. In December 2021, Massachusetts ended its program of widespread contact tracing, at least in part due to the program's high costs and limited effectiveness in the face of new COVID-19 variants.[4] Dozens of other States have likewise ended their contact-tracing programs in recognition of their limited efficacy.[5] Governor Hochul of New York, for example, ended her

[2] Jill McKeon, *COVID-19 Contact Tracing Had Little Impact on Public Health*, Health IT Analytics (June 9, 2021), available at https://healthitanalytics.com/news/covid-19-contact-tracing-had-little-impact-on-population-health (last visited Nov. 8, 2022).

[3] Caitlin Owens, *Contact Tracing Fizzles Across America*, Axios (Jan 28, 2022), available at https://www.axios.com/2022/01/28/coronavirus-contact-tracing-public-health-omicron (last visited Nov. 8, 2022).

[4] Kay Lazar, *Nearly $160 million Later, the State's COVID-19 Contact Tracing Program Is Ending*, Bos. Globe (Dec. 16, 2021), available at https://www.bostonglobe.com/2021/12/16/metro/nearly-160-million-later-states-covid-19-contact-tracing-program-is-ending/ (last visited Nov. 8, 2022).

[5] *Id.*

State's contact-tracing program in January 2022, explaining that "contact tracing methods used earlier in the pandemic are no longer effective in disrupting transmission chains."[6]

13. In March 2022, the Centers for Disease Control and Prevention dropped its recommendation for widespread contact tracing of the entire populace.[7]

14. On September 18, 2022, President Biden announced on *60 Minutes* that "[t]he pandemic is over."[8]

II. DPH WORKED WITH GOOGLE TO DEVELOP ITS CONTACT TRACING APP AND TO INSTALL THE APP ONTO MILLIONS OF ANDROID DEVICES WITHOUT OWNERS' AWARENESS OR PERMISSION

15. While DPH's contact-tracing program was still in effect, it developed and deployed mobile device applications to assist contact-tracing efforts.

16. In May 2020, Google and Apple Inc. ("Apple") developed a mobile device API that serves as a framework to enable public health authorities to develop their own mobile contact-tracing apps.[9] The Google API is used to develop contact-tracing apps for the Android operating system, and the Apple API is used for iOS devices.

---

[6] Karen DeWitt, *NY Ends Contact Tracing, Saying It's Not Effective Against Omicron*, WXXI News (Jan. 12, 2022), available at https://www.wxxinews.org/capitol-bureau/2022-01-12/ny-ends-covid-contact-tracing-saying-its-not-effective-against-omicron (last visited Nov. 8, 2022).

[7] *C.D.C. Drops Contact Tracing Recommendation*, N.Y. Times (Mar. 2, 2022), available at https://www.nytimes.com/live/2022/03/02/world/covid-19-tests-cases-vaccine (last visited Nov. 8, 2022).

[8] David Cohen & Adam Cancryn, *Biden on '60 Minutes': 'The Pandemic is over,'* Politico (Sept. 18, 2022, 8:47 PM), available at https://www.politico.com/news/2022/09/18/joe-biden-pandemic-60-minutes-00057423 (last visited Nov. 8, 2022).

[9] David Burke, *An Update on Exposure Notifications*, Google (July 31, 2020), available at https://blog.google/inside-google/company-announcements/update-exposure-notifications (last visited Nov. 8, 2022).

17. According to Google and Apple's joint statement: "What we've built is not an app—rather public health agencies will incorporate the API into their own apps that people install."[10] With respect to Android devices, COVID-19 contact tracing would not occur unless the device owner were to "install or finish setting up a participating app" from a public health agency.[11]

18. By April 2021, public health agencies in Alabama, Arizona, California, Colorado, Connecticut, Delaware, the District of Columbia, Guam, Hawaii, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, , Utah, Virginia, Wyoming, Washington, and Wisconsin had released their own contact-tracing apps using the Google API for installation on Android devices.[12]

---

[10] Google & Apple, *Exposure Notification API Launched to Support Public Health Agencies* (May 20, 2020), available at https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/(last visited Nov. 8, 2022). A number of device owners expressed concern on social media and elsewhere that Google and Apple had secretly installed COVID-19 tracking apps on their devices without permission, but this view appears to have been mistaken. Google's and Apple's APIs were not an app but rather a framework to help public health agencies develop their own apps. *See* McKenzie Sadeghi, *Fact Check: Google Did Not Automatically Sign Up Android Users for COVID-19 Tracing App*, USA Today (June 14, 2020), available at https://www.usatoday.com/story/news/factcheck/2020/06/14/fact-check-android-users-must-opt-into-covid-19-tracing-technology/5341250002/ (last visited Nov. 8, 2022).

[11] Davey Winder, *Have Apple and Google Uploaded a COVID-19 Tracking App To Your Phone? The Facts Behind the Furor*, Forbes (July 20, 2020), available at https://www.forbes.com/sites/daveywinder/2020/06/20/have-apple-and-google-suddenly-uploaded-a-covid-19-tracking-app-to-your-phone-android-iphone-exposure-notification-contact-tracing/?sh=322aed060545 (last visited Nov. 8, 2022) (displaying screenshot of Android device stating that COVID exposure notifications do not activate unless device owner "install[s] or finish[es] setting up a participating app").

[12] Matthew Sholtz, *COVID Tracking App Roundup: All of the Countries and US States that Currently Offer Exposure Notification App*, Android Police(Apr. 1, 2021), https://www.androidpolice.com/2021/01/02/covid-tracing-apps-ens-android/ (last visited Nov. 8, 2022).

19. Several foreign countries also developed and deployed contact-tracing apps using the Google API for installation on Android devices.[13] Australia's Department of Health, for instance, used Google's API to develop an app called COVIDSafe for Android devices.[14] A government-funded study published in February 2022 found that Australia's nationwide contact-tracing app was unhelpful and ineffective in the country's COVID-19 pandemic response.[15]

20. Massachusetts DPH developed two versions of its contact-tracing apps for use on Android devices using the Google API.

21. The first version, labeled "MassNotify" in the Google Play Store, became available in or around April 2021 and—like other States' apps—requires an Android user to affirmatively install. It also appeared as an icon on the device's home screen. According to the Google Play Store, as of November 8, 2022, this version of MassNotify has been installed by only approximately 5,000 Android users and has 50 reviews, several of which complain of the version's low rate of adoption.[16] For example, one reviewer stated in May 2021 that "[i]f adoption were

---

[13] Bobbie Johnson, *The Covid Tracing Tracker: What's Happening in Coronavirus Apps Around the World*, MIT Tech. Rev. (Dec. 16, 2020), available at https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker/ (last visited Nov. 8, 2022).

[14] Australia also used Apple's API to develop a COVIDSafe app for use on Apple devices. *See COVIDSafe App*, Austl. Gov't Dep't Health & Aged Care (Aug. 26, 2022), available at https://www.health.gov.au/resources/apps-and-tools/covidsafe-app (last visited Nov. 8, 2022).

[15] Florian Vogt, et al., *Effectiveness Evaluation of Digital Contact Tracing for COVID-19 in New South Wales, Australia*, 7 Lancet Pub. Health e250 (2022), available at https://www.thelancet.com/action/showPdf?pii=S2468-2667%2822%2900010-X (last visited Nov. 8, 2022).

[16] Google Play, MassNotify, developed by MA Department of Public Health, available at: https://play.google.com/store/apps/details?id=gov.ma.covid19.exposurenotifications (last visited Nov. 8, 2022).

wider, this app might be more useful," and another complained in June 2021 that "[i]t appears no one else uses the app except my immediate family."[17]

22. This initial version of MassNotify is no longer being maintained and is not functional. On January 20, 2022, a reviewer stated that she "tried to enter a positive self test and I had no way to get a verification code."[18] Another April 26, 2022 reviewer stated "When I try to report a positive test it requests a Verification code? However, none is sent to my phone or email address and there seems to be no way to request one be sent."[19]

23. The second version was originally labelled "MassNotify v.3" in the Google Play Store,[20] but has since been re-branded as "Exposure Notification Settings Feature–MA." This version is referred to herein as DPH's Contact Tracing App. Instead of making the Contact Tracing App available for voluntary download, however, starting on or around June 15, 2021, DPH worked with Google to "automatically distribute[]" the App to Android devices "so users don't have to download a separate app."[21] In other words, the Contact Tracing App was installed onto Android mobile devices without users' permission or awareness. Upon information and belief, DPH and Google developed the revised App in order to overcome Android users' low rate of voluntary

[17] *Id.* (reviews of Bryant Finney and Obed Oby Almeyda).

[18] *Id.* (review of Katie Rabbitt).

[19] *Id.* (review of Chris Phillips).

[20] Ron Amadeo, *Even Creepier COVID Tracking: Google Silently Pushed App to Users' Phones*, Ars Technica (June 21, 2021), available at https://arstechnica.com/gadgets/2021/06/even-creepier-covid-tracking-google-silently-pushed-app-to-users-phones/ (last visited Nov. 8, 2022) ("There are two versions of the 'MassNotify' app on the Play Store. … A second version [is] labeled 'v3' in the package name[.]").

[21] *Id.*

adoption of the initial App. According to the Google Play Store, DPH's Contact Tracing App was installed onto over one million Android.[22] On information and belief, the overwhelming majority of these installs were surreptitious.

24. The Contact Tracing App is identical to the initial MassNotify app except that it installs **without device owners' permission**. As one Google Play review explained on June 19, 2021: there are "2 different entries of this app on the playstore, one autoinstalled on my device without permission overnight. I did some research finding myself on this [initial] one where I am still able to install on my phone at the same time as the other that looks exactly like this, other than the reviews and downloads. This is highly weird and disrespectful of our privacy. I wouldn't trust the app at all."[23]

25. Once "auto-installed," DPH's Contact Tracing App does not appear alongside other apps on the Android device's home screen. Rather, the App can be found only by opening "settings" and using the "view all apps" feature.[24] Thus, by design, the typical device owner would remain unaware of its presence.

26. On information and belief, DPH decided to secretly install the Contact Tracing App onto over one million Android devices because its initial version, which required voluntary download, was not being widely adopted by Massachusetts citizens by June 2021. Rather than

---

[22] Google Play, Exposure Notification Settings Feature – MA, developed by MA Department of Public Health , available at: https://play.google.com/store/apps/details?id=gov.ma.covid19.exposurenotifications.v3 (last visited Nov. 8, 2022).

[23] MassNotify Comments, *supra* note 16 (review of Josh Ciares).

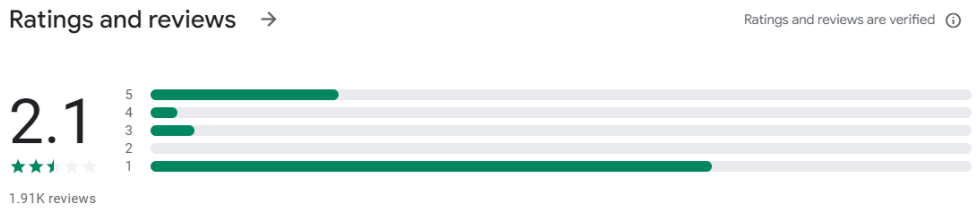
[24] Abner Li, *Massachusetts 'MassNotify' Android App Auto-Installed, But COVID Exposure Alerts Are Not Enabled*, 9to5Google (June 19, 2021, 12:29 PM), available at https://9to5google.com/2021/06/19/massachusetts-massnotify-app/ (last visited Nov. 8, 2022).

implement an awareness campaign to encourage voluntary adoption, like other States did, DPH took a shortcut and mass-installed the App without device owners' awareness or permission.

27. On information and belief, DPH used cell site location information ("CSLI") to target all Android devices located in or transported through the Commonwealth of Massachusetts for installation.

28. No law or regulation authorizes DPH to install any type of software—let alone what amounts to spyware designed to obtain location and health information—onto the Android devices of Massachusetts residents without their awareness or permission.

29. As of September 22, 2022, there are approximately 1,900 reviews of DPH's Contact Tracing App on the Google Play Store, the vast majority of which are lowest-possible one-star ratings.[25] A screenshot of the distribution of reviews taken on November 8, 2022, shows the following:



30. Reviewers complain that, without permission, the App downloaded onto their mobile devices, turning on the Bluetooth—likewise without permission—and hiding itself in "settings" instead of appearing as an icon alongside all other apps on the device. Some illustrative examples are listed below:

[25] Reviews found on Google Play, Exposure Notification Settings Feature – MA, developed by MA Department of Public Health [hereinafter Contact-Tracing App Reviews], available at: https://play.google.com/store/apps/details?id=gov.ma.covid19.exposurenotifications.v3 (last visited on Nov. 8, 2022). Screenshots of quoted reviews are attached as Exhibit 1.

a. "I absolute did not install this on my phone. It was silently installed without notification. It doesn't have an app icon—you have to go through settings and view all apps. This is a huge privacy and security overstep."

b. "As with other people, this was downloaded without my knowledge or permission, but on my Samsung tablet, which has not traveled to Massachusetts. Only saw it because my internet protection program is set up to ask to scan new apps."

c. "SPYWARE?! Automatically installed without consent. It has no icon, no way to open this and see what it even does, which is a huge red flag. Per the notifications it runs on Bluetooth which is a major battery drain, and seems to want to track my location."

d. "I always turn off data, location and Bluetooth on this phone because I have VERY limited data, by my own CHOICE, but those settings kept getting turned on in the past few days, so i went into 'my apps' to check why and TADAAA!! Whaddayaknow, this app is the culprit! And it installed SILENTLY!? This could have cost me a LOT of $$ had I not figured it out, like most people probably won't!?"

e. "I hate this app. This downloaded onto my device without me noticing and now I am getting notifications everyday from it telling me to turn it's [*sic*] service on. I can't even open it with an icon!"

f. "I never installed this and never saw it until I went in to update apps. It definitely installed on its own and I believe I caught the tail end of it installing one day when I saw something saying finish installing and I could never find out what that was."

g. "I can't believe I just found this app on my phone. This app downloaded itself onto my phone. I did NOT give Google or any authority permission to do so. I also never opted into the Android Covid-19 notification program. This is ridiculous and utterly unacceptable."

h. "Did not install - Appeared on my phone without my consent and I didn't download. This is not acceptable. I understand the premise and well meaning behind the app - but again - my cell phone is MY personal property and the thought of someone (or the government) to think their app is so important to just auto-install it on my phone hit every level of audacity. Shame on you."

i. "Omg!!!! This app somehow installed itself on my phone. I uninstalled it and went to free up some space by getting rid of apps i dont really use, and it had already reinstalled itself. After i post this, I[] bet it will have reinstalled again. This app is harder to get rid of than Covid."[26]

[26] *Id.* (reviews of Shauna McCarthy, C M, Callie M, Dawn Driscoll, EggStopper5, Karla Murray, Eliz, Doreen Gamache, and Kathleen Kenneally).

31. DPH began secretly installing its Contact Tracing App onto Android mobile devices owned by individuals who reside in or travel to or through Massachusetts on or around June 15, 2021. On information and belief, DPH continues to secretly install the App onto Android devices without obtaining owners' permission or awareness. For example, on September 18, 2022, a one-star review on Google Play stated that he or she "[d]idnt even install it" and that DPH's Contact Tracing App "[j]ust showed up."[27] Another complained on September 14, 2022: "Every time something COVID related has come up on my phone, I have denied permission and opted out. I went to update a different app and found this had been installed and had an update as well. I promptly uninstalled it. I wonder where the legality lies."[28]

32. On information and belief, DPH periodically installs the App onto all Android devices located in or being transported through Massachusetts. To accomplish the stealth installations of the Contact Tracing App, DPH uses an Android device's location data to target individuals who happen to be in Massachusetts. As a result, individuals who reside in other States but travel to or through Massachusetts, such as Plaintiffs, will have the App installed on their Android devices. For instance, one Google Play reviewer stated: "I am not a Massachusetts resident and this spyware was surreptitiously installed on my phone without my consent or notification. It keeps reinstalling itself after removal. Words cannot describe how violated this makes me feel both from MA and Google."[29]

---

[27] *Id.* (review of Corie W).

[28] *Id.* (review of Brandon Engle).

[29] *Id.* (review of S-ro Sorcxisto); *see also id.* (review of David Lee) ("I work in Massachusetts but live in another state. I wouldn't even have known about this app if I hadn't read a story on The Liberty Daily about how the Massachusetts Department of Public Health is installing it without

33. Even after a device owner uninstalls the App, the App "keeps reinstalling itself after removal."[30] A March 31, 2022, reviewer complained that "[t]his app installed itself secretly and I have uninstalled it multiple times for it to keep reinstalling itself!"[31] Another reviewer said that she "removed it and it reinstall[ed] itself."[32]

34. Because the App does not appear as an icon on the Android devices' home screen, several reviewers expressed confusion regarding how to uninstall the App even after they discovered its presence. For example, multiple reviewers stated they do not know how to uninstall the app even after they learned of the App's existence.[33] On information and belief, a significant portion of the over one million individuals on whose devices the App was secretly installed

---

people's permission and searched for it. As others have said there is no icon in the menu, you have to search for it in the app portion of settings."); *id.* (review of Joe Kivel) ("I don't live in Massachusetts. I don't work in Massachusetts. I visited the state for four days this past week. And the app was installed on my phone without my permission or knowledge. Had I not read the article on Android Police I would not have searched my phone for it."); *id.* (review of Jason Lee) ("Why am I being prompted to update or uninstall an app I never installed in the first place. I am not from Massachusetts and have not been there in years."); *id.* (review of Maxine Kylaa) ("Did not install this, don't live in MA.").

[30] *Id.* (review of S-ro Sorcxisto).

[31] *Id.* (review of Elisa Bennett).

[32] *Id.* (review of Beth Silvaggio); *see also id.* (review of Mike C.) ("This is definitely not okay that you cannot even uninstall this app as it reinstalls itself."); *Id.* (review of Branden Dion) ("Update: just found it reinstalled AGAIN WITHOUT MY PERMISSION."); *id.* (review of Scott) ("Like others a sneak attack installation and after I uninstalled IT INSTALLED AGAIN!").

[33] *Id.* (review of Shelby Christian) ("I can't get it to uninstall."); *id.* (review of Torchcat) ("[I]nstalling apps to a person's phone without permission and with no way to uninstall or disable said app is bull."); *id.* (review of Michael Donato) ("I did not consent to it being installed. I[t] cannot be uninstalled."); *id.* (review of Thomas Galant) ("Couldn't find a[n] icon to uninstall it so I had to go into settings then apps to uninstall it.").

remains ignorant of the App's presence or unaware of how to uninstall the App. This is by deliberate design.

35. While other States have also used Google's API to develop contact tracing applications for Android Devices, those other States do not secretly install their apps without device owners' permission or awareness. Reviews of Virginia Department of Health's app, COVIDWISE, for instance, do not complain of secret and non-consensual installations.[34] Nor do reviewers of New York's COVID Alert NY app, even though there may be as many downloads of COVID Alert NY as DPH's Contact Tracing App.[35]

III. DPH'S CONTACT TRACING APP EXPOSES MOVEMENT AND PERSONAL CONTACT INFORMATION

36. DPH's Contact Tracing Apps generates for each mobile device a random "Rolling Proximity Identifier" every 15 to 20 minutes.[36] The App causes the mobile device to broadcast the Identifier via Bluetooth to other Bluetooth-enabled devices within range.

---

[34] *See* Google Play, COVIDWISE, developed by the Virginia Department of Health, available at https://play.google.com/store/apps/details?id=gov.vdh.exposurenotification&hl=en_US&gl=US (last visited Nov. 8, 2022).

[35] *See* Google Play, COVID Alert NY, Developed by the New York State Department of Health, available at https://play.google.com/store/apps/details?id=gov.ny.health.proximity (last visited Nov. 8, 2022) (indicating over one million downloads).

[36] *Exposure Notification: Bluetooth Specification*, Google (Apr. 2020), available at https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf/ (last visited Sept. 22, 2022);*Exposure Notification: Cryptography Specification*, Google (Apr. 2020), available at https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf/ (last visited Nov. 8, 2022).

37. The App also causes the mobile device to broadcast a MAC address via Bluetooth, which is a sequence of characters that identifies a device on a network.[37] Each mobile device has a MAC address that can be used to identify the owner.

38. MAC addresses are also readily associated with specific locations. For example, an open-source project called "Wigle" maintains a publicly searchable database associating MAC addresses with specific locations.[38] Thus, knowing when an individual's device connected with a MAC address associated with a specific location—such as a store—would provide knowledge of the device owner's location at a particular time. And a series of such data points would provide a reasonably precise timeline of the device owner's movement.

39. The App also causes the user's mobile device to receive RPIs and MAC addresses that are broadcast by other devices within Bluetooth range.

40. The App records all RPIs and MAC addresses that it broadcasts and receives, along with the precise time and estimated distance from the source based on the Bluetooth signal strength.

41. Android devices host a "system log" for logging device metrics, which application developers, device manufacturers, and network operators use for evaluation purposes.

42. System log files enable application developers and others to obtain data for evaluating the stability and reliability of their applications. As such, the system logs exist to transmit information in the logs from the phone to certain application developers.

---

[37] *Media Access Control Address (MAC Address)*, Techopedia (Nov. 18, 2014), available at https://www.techopedia.com/definition/5301/media-access-control-address-mac-address (last visited Nov. 8, 2022).

[38] Wigle, https://wigle.net (last visited Sept. 22, 2022); *see also* MAC Address Vendor Lookup, https://macaddress.io/ (last visited Nov. 8, 2022).

43. Android system log files are transmitted to application and operating system developers, device manufacturers, and network providers in the ordinary course of the phones' operation. For example, system log data is commonly transmitted as part of "crash reporting." When an application unexpectedly stops working, the system log will be transmitted to the developer to inspect and identify errors.

44. The system log of each mobile device contains personal identifying information, including the smartphone's permanent MAC address and its "name." Other identifiers include the name of wireless networks to which the device connects, the MAC address of the wireless network router to which the device connects, and the email address of the device owner's Google account. According to research on the Google API funded by the Department of Homeland Security: "An entity that collects logs can also be associated [a MAC address] to the user's identity," in part because such an entity could "get the email and phone number of a device, [and] there are other persistent identifiers that can be accessed as well."[39]

45. For mobile devices on which DPH's Contact Tracing App is installed, RPIs and MAC addresses broadcast and received by the device are placed on the system log. An entity with access to system logs of multiple devices would know which MAC addresses are associated with each device and thus could determine when individual device owners were in close proximity with one another. An entity with access to a device's system log could further correlate received MAC

[39] Joel, Reardon, *Why Google Should Stop Logging Contact-Tracing Data*, AppCensus Blog (Apr. 27, 2021), available at https://blog.appcensus.io/2021/04/27/why-google-should-stop-logging-contact-tracing-data/(last visited Sept. 22, 2022).

addresses with MAC addresses associated with known fixed locations, thereby determining where the device owner has been.[40]

46. In sum, an entity with access to the system log of a mobile device on which the Contact Tracing App is installed would be able to identify the owner of the device by inspecting the phone's MAC address, email, phone name, and other non-random identifiers in the system log. The entity would also have a historical record of MAC addresses of other individuals and locations to which the device owner had been in close proximity. This information enables a person with access to identify the device owner and construct a timeline of locations where he or she has travelled and of individuals with whom the device owner has been in close contact.

47. On information and belief, the Contact Tracing App gives DPH access to system logs of Android devices on which the App is installed, allowing DPH (and potentially others) to identify device owners and determine their past movement and personal contacts, all without their consent.

48. On information and belief, countless other app developers have access to system logs of Android devices.[41] By installing the Contact Tracing App on an Android device without

[40] *Id.* ("An entity that collects users logs can turn the RPI they hear into the corresponding MAC address; with access to existing databases, they can turn the MAC address into a geolocation. This allows them to learn a location history of a user based on geolocating the RPIs they hear.").

[41] For example, Samsung's privacy policy states that "information we may collect automatically includes information about: your device, including MAC address, IP address, log information …." *Samsung Privacy Policy for the U.S.*, Samsung (Oct. 1, 2021), available at https://www.samsung.com/us/account/privacy-policy/(last visited Sept. 22, 2022); Xiaomi, a Chinese electronics company that develops smartphones and apps, likewise states in its privacy policy that it collects "standard system logs" from customers. *Xiaomi Privacy Statement* (Jan. 15, 2021), available at https://privacy.mi.com/all/en_US/ (last visited September 22, 2022). Facebook and Instagram also explicitly state that they collect "unique identifiers, device IDs and other identifiers, such as from game, apps or accounts you use." *Instagram Data Policy*, Meta (Jan. 4, 2022), available at https://help.instagram.com/155833707900388/ (last visited September 22, 2022); *Privacy Policy*, Meta (July 26, 2022), available at

its owner's awareness or permission, DPH exposes that device owner's past movements and personal contacts to these other developers with system log access.[42]

49. In April 2021, users of Android contact-tracing apps developed using Google's API filed a class action lawsuit against Google alleging that such apps "leav[e] users' private health information unprotected on Android device 'system logs' to which Google and third party app developers had routine access." Brief in Support of Preliminary Settlement Approval at 4, *Diaz v. Google LLC*, No. 5:21-cv-03080-NC (N.D. Cal. May 6, 2022), ECF No. 64. Google agreed to settle that lawsuit in May 2022. *Id.* at 9.

50. Even though the App is downloaded and collects data without user permission or awareness, the device owner must enable the exposure notification functionality to join DPH's COVID-19 reporting system.[43]

51. Even if an App user does not enable exposure notification, his or her mobile device would still broadcast and receive Bluetooth signals and record MAC addresses of other Bluetooth devices with which he or she comes into contact.[44] This information is saved on the mobile

---

https://www.facebook.com/about/privacy (last visited Nov. 8, 2022) (collecting "identifiers that tell your device from other users'").

[42] Nicole Wetsman, *Android Bug Exposed COVID-19 Contract Tracing Logs to Preinstalled Apps*, Verge (Apr. 27, 2021, 10:20 AM), available at https://www.theverge.com/2021/4/27/22405425/android-google-contact-tracing-bug-privacy (last visited Nov. 8, 2022) ("The Android version of Google and Apple's COVID-19 exposure notification app had a privacy flaw that let other preinstalled apps potentially see sensitive data").

[43] If an App user enables exposure notification and reports a positive COVID-19 diagnosis, that result is submitted through DPH's Contact Tracing App. On information and belief, the user's Keys are uploaded to a server maintained by DPH, and the user is designated as COVID-19 infected. DPH's App then uses the record of RPIs that the infected user has come into contact with over the past fourteen days and sends exposure notifications regarding the date, duration, and distance of the exposure to other App users corresponding to those RPIs.

[44] Numerous Google Play reviewers complain that the App causes their Android devices to broadcast over Bluetooth without their permission. *See, e.g.*, Contact-Tracing App Reviews, *supra*

device's system log, and anyone, including DPH, with access to the log would be able to retrace the App user's past location and contacts.

52. On May 27, 2020, Arizona filed a lawsuit against Google alleging that "individual users of Google products and services are the targets of a sweeping surveillance apparatus designed [by Google] to collect their behavioral data *en masse*, including data pertaining to user location." Redacted Complaint ¶ 6, *State of Arizona v. Google LLC*, No. CV2020-006219 (AZ Super. Ct. May 27, 2020).[45] On October 4, 2022, Google agreed to pay an $85 million settlement to resolve Arizona's claims that it illegally tracked the location of Android device users. Malathi Nayak, Google to Pay $85 Million to End Arizona Consumer-Privacy Suit, Bloomberg (Oct. 4, 2022).[46]

53. On January 24, 2022, Attorneys General from Washington D.C., Indiana, Texas, and Washington also filed separate lawsuits against Google alleging "that the search giant deceived consumers to gain access to their location date."[47] The Washington D.C. lawsuit, for instance,

---

note 25 (review of David Greiner) ("Installed without consent. Completely messed up my Bluetooth and I couldn't figure out what was going on until I uninstalled this."); *id.* (review of Dawn Driscoll) ("I always turn off data, location and Bluetooth on this phone because I have VERY limited data, by my own CHOICE, but those settings kept getting turned on in the past few days, so i went into 'my apps' to check why and TADAAA!! Whaddayaknow, this app is the culprit! And it installed SILENTLY!"); *id.* (review of Laura) ("Why did the state I live in install an app on my phone without my permission? The app is completely useless, and yet it demands my location and sucks up my battery life using Bluetooth."). Screenshots of quoted reviews are attached as Exhibit 1.

[45] Available at: https://www.azag.gov/sites/default/files/2021-05/Complaint%20%28redacted%29.pdf

[46] Available at: https://www.bloomberg.com/news/articles/2022-10-04/google-to-pay-85-million-to-end-arizona-consumer-privacy-suit?sref=ExbtjcSG (last visited Nov. 8, 2022).

[47] Cat Zarkrezwski, Google deceive consumers about how it profits from their location data, attorneys general allege in lawsuits, Washington Post (Jan. 24, 2022), available at: https://www.washingtonpost.com/technology/2022/01/24/google-location-data-ags-lawsuit/ (last visited Nov. 8, 2022).

claims that "[s]ince at least 2014, Google deceived consumers regarding how their location is tracked and used[.]" Complaint for Violations of the Consumer Protection Procedure Act ¶ 2, *District of Columbia v. Google, LLC*, No. 2022 CA 000330 B (D.C. Super. Ct. Jan. 24, 2022).[48] According to these that complaint, "[t]hrough sensors and APIs installed on Android Devices, Google can track the precise location of a device on a continuous basis." *Id.* ¶ 21 (footnote omitted). When a "device scans for nearby Wi-Fi access points or Bluetooth devices, [it] can help Google interpret the user's location." *Id.* ¶ 43.

54. Despite being aware of these privacy and consumer-protection allegations concerning Google's API and Bluetooth scans, DPH continues to secretly install the Contact Tracing App, which is based on Google's API and enables Bluetooth scans, onto Android devices without their owners' consent or awareness.

IV. SECRET INSTALLATION OF DPH'S CONTACT TRACING APP IS STATE ACTION

55. State action is established when there is "sufficiently close nexus between the State and the challenged action of the [private] entity so that the action of the latter may be fairly treated as that of the State itself." *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 351 (1974); *see also Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government." (collecting cases)); *United States v. Feffer*, 831 F.2d 734, 737 (7th Cir. 1987)

[48] Available at: https://oag.dc.gov/sites/default/files/2022-01/DCv.Google%281-24-22%29.pdf (last visited Nov. 8, 2022).

("The government may not do, through a private individual, that which it is otherwise forbidden to do.").

56. The downloading of the Contract Tracing App onto Android devices constitutes state action. Massachusetts DPH developed the app using API provided by Google, and Google has explicitly stated that its employees "have been working with the Massachusetts Department of Public Health" to ensure the App would be "automatically distributed" onto Android devices."[49] These "clear indices of Government's encouragement, endorsement, and participation" demonstrates that Google acted as an instrumentality of DPH when it installed DPH's Contact Tracing App onto millions of Android devices without their owners' permission or awareness. *Skinner*, 489 U.S. at 614.

V. SECRET INSTALLATION OF DPH'S CONTACT TRACING APP CAUSES PLAINTIFFS CONCRETE AND IRREPARABLE HARM

57. Defendants' actions have caused, and will continue to cause, Plaintiffs to suffer concrete and irreparable harm.

58. Plaintiffs have constitutional interests in not having their whereabouts and contacts surveilled, recorded, and broadcast.

59. Plaintiffs also have constitutional and common-law property interests in not having an app, especially one that they did not want or agree to have installed, use up the Plaintiffs' monthly data allowances for their mobile devices (smartphones and tablets) or drain the batteries by having their devices be forced to broadcast Bluetooth signals.

[49] Li, *supra* note 24

60. Plaintiffs also have an interest in preventing unauthorized and unconsented to access to their personal Android devices by government agencies and others, particularly where such access is for the purpose of obtaining information from them (*i.e.*, conducting a search).

61. Defendants worked with Google to download the App onto mobile devices without device owners' permission or knowledge, merely because those device owners happened to live in or be travelling through Massachusetts.

62. This App tracks Plaintiffs' whereabouts and contacts and records data that allows the State to retrace their movement over a long period of time. This is true even if Plaintiffs do not enable the App's exposure notification feature. When Plaintiffs deleted the Contact Tracing App, DPH surreptitiously re-installed it onto their Android devices. Plaintiffs expect that the process will repeat should they attempt to delete the Contact Tracing App again.

63. Accordingly, Defendants' actions have caused and will continue to cause Plaintiffs irreparable harm, including but not limited to the loss of their constitutional and common-law rights to privacy and property and the unauthorized access to their personal Android devices.

VI. CLASS ALLEGATIONS

64. Plaintiffs bring this action on behalf of the following class: All persons in the United States on whose smartphones or mobile devices DPH, working with Google, installed its Contact Tracing App without the device owner's permission.

65. The prerequisites of maintaining a class action under Federal Rule of Civil Procedure 23(a) are satisfied:

a. *Numerosity*: the class of individuals on whose mobile devices the App was secretly downloaded exceeds one million members.

b. *Commonality*: common questions of law and facts apply to all class members because they have been injured by the same illegal conduct, *i.e.*, secret installation of spyware onto their mobile devices that enable location tracking. These common questions are susceptible to common answers.

c. *Typicality*: the claims of the named Plaintiffs are the same as those of the class members.

d. *Adequacy*: the named Plaintiffs have no conflicts of interest and counsel have requisite experience to represent the class.

66. The prerequisites of maintaining a class action under Federal Rule of Civil Procedure 23(b)(2) are satisfied because DPH's unlawful action applies to the entire class, and Plaintiffs seek injunctive and declaratory relief, along with nominal damages, with respect to the class as a whole.

CLAIMS FOR RELIEF

Count I: 42 U.S.C. § 1983 - Violation of the Fourth Amendment to the U.S. Constitution

67. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

68. The U.S. Constitution protects individuals from unreasonable searches and seizures by government actors. *See* U.S. Const. amend. IV. The Fourth Amendment is incorporated against the States. *See Mapp v. Ohio*, 367 U.S. 643, 660 (1961).

69. The Fourth Amendment applies when a private party acts as an instrument or agent of the government. *See Skinner*, 489 U.S. at 614.

70. A Fourth Amendment search occurs when government action intrudes into an individual's reasonable expectation of privacy. *California v. Ciraolo*, 476 U.S. 207, 211 (1986);

United States v. Jacobsen, 466 U.S. 109, 113 (1984). "[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [digital surveillance]." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). Mapping a mobile device's location history creates an "all-encompassing record" of the owner's whereabouts and constitutes a Fourth Amendment violation. *Id.*

71. No different from *Carpenter*, here, DPH's App enables location tracking of an Android phone by the Commonwealth of Massachusetts and thus constitutes a Fourth Amendment search. The Commonwealth is indiscriminately conducting a search of all individuals with Android devices who reside in or have passed through Massachusetts between June 15, 2021, and present day. These searches constitute clear Fourth Amendment violations.

72. A Fourth Amendment search also occurs "when the government: (1) trespasses upon a constitutionally protected area, (2) to obtain information." *Taylor v. City of Saginaw*, 922 F.3d 328, 332 (6th Cir. 2019) (citing *United States v. Jones*, 565 U.S. 400, 404 (2012)).

73. DPH has secretly installed an unwanted App onto the Android devices of over a million individuals for the purpose of gathering information about those individuals. Each such installation is a trespass to obtain information and thus constitutes a Fourth Amendment search. These searches constitute clear Fourth Amendment violations.

74. 42 United States Code § 1983 provides a cause of action for any person whose Constitutional rights are violated by state action.

75. Accordingly, Defendants' illegal and unconstitutional installation of the Contact Tracing App must be enjoined and set aside. *See* U.S. Const. amend. IV.

Count II: Violation Article XIV of the Massachusetts Declaration of Rights

76. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

77. Article XIV of the Massachusetts Declaration of Rights provides individuals with "a right to be secure from all unreasonable searches." Mass. Const. pt. I, § I, art. XIV. "Privacy rights under [Article XIV] are at least as extensive as those under the Fourth Amendment." *Garcia v. Commonwealth*, 486 Mass. 341, 350 (2020).

78. A search occurs under Article XIV when an individual has a subjective expectation of privacy, and that expectation of privacy is one that society views as reasonable. See *Commonwealth v. Augustine*, 467 Mass. 230, 241 (2014). Obtaining an individual's location and personal data from a mobile device is a search. *Id.* at 255.

79. DPH's Contact Tracing App indiscriminately obtains location data from Android devices and thus implements searches in clear violation of Article XIV.

80. "Regardless of whether there is an intrusion on a reasonable expectation of privacy, a search also occurs when the government … obtains information by physically intruding on persons, houses, papers of effects[.]" *Garcia*, 486 Mass. at 350 (quotation marks and citation omitted).

81. Android devices are "effects" protected under Article XIV. DPH intruded on such effects when it worked with Google to secretly install its Contact Tracing App onto citizens' Android devices without their awareness or permission. Such installations thus constitute searches in clear violation of Article XIV.

82. Accordingly, Defendants' illegal and unconstitutional installation of its Contact Tracing App must be enjoined. *See* Mass. Const. pt. I, § I, art. XIV.

Count III: 42 U.S.C. § 1983 - Uncompensated Takings in violation of the Fifth Amendment to the U.S. Constitution

83. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

84. The U.S. Constitution protects individuals from having their private property "taken for public use, without just compensation." U.S. Const. amend. V. The Takings Clause has been incorporated against the States.

85. A *per se* taking occurs when the government effects a "physical occupation of property," even if the occupied space is small and there is "minimal economic impact." *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 434 (1982); *see also Cedar Point Nursery v. Hassid*, 141 S. Ct. 2063, 2066, 2072 (2021).

86. The "physical occupation" principle applies where the government occupies digital storage space of an individual's mobile device. A taking occurs—and compensation is due— even when the amount of digital storage space taken is small, the duration is temporary, and the economic impact is minimal.

87. DPH occupied the digital storage of private mobile devices when it worked with Google to secretly install its Contact Tracing App onto citizens' mobile devices.

88. The secret installation of the Contact Tracing App constitutes a taking under the Fifth Amendment for which just compensation is due but was never offered nor provided.

89. 42 United States Code § 1983 provides a cause of action for any person whose Constitutional rights are violated by state action.

90. Accordingly, Defendants' conduct should be declared an uncompensated and thus unconstitutional taking of private property. *See* U.S. Const. amend. V.

Count IV: Uncompensated Appropriation under Article X of the Massachusetts Declaration of Rights

91. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

92. Article X of the Massachusetts Declaration of Rights states that "whenever the public exigencies require that the property of any individuals should be appropriated for public uses, he shall receive a reasonable compensation thereof." Mass. Const. pt. I, § I, art. X.

93. "Appropriating a portion of property … is nonetheless an appropriation requiring compensation." *Dimino v. Sec'y of Com.*, 427 Mass. 704, 709 n.5 (1998) (citing *Loretto*, 458 U.S. at 430).

94. DPH appropriated the digital storage of private mobile devices when it worked with Google to secretly install its Contact Tracing App onto citizens' mobile devices. This installation constitutes an appropriation under Article X for which reasonable compensation is due.

95. Accordingly, Defendants' conduct should be declared to be an appropriation of private property for which compensation is required. *See* Mass. Const. pt. I, § I, art. X.

Count V: *Ultra Vires* Government Action

96. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

97. "[A] state officer may be said to act *ultra vires* [] when he acts 'without any authority whatever.'" *N.H. Ins. Guar. Ass'n v. Markem Corp.*, 424 Mass. 344, 353 (1997).

98. Moreover, a state "agency may not exceed those powers and obligations expressly conferred on it by statute or reasonably necessary to carry out the purposes for which the statute was enacted." *Mass. Fed'n of Tchrs., AFT, AFL-CIO v. Bd. of Educ.*, 436 Mass. 763, 773 (2002).

99. An agency's *ultra vires* conduct is void and must be enjoined. *See New England Power Generators Ass'n, Inc. v. Dep't of Env't Prot.*, 480 Mass. 398, 407-08 (2018).

100. No statute authorizes DPH to install software of any sort onto individuals' mobile devices without their consent or awareness, let alone secretly install the Contact Tracing App that exposes location and personal data. To the contrary, such secret installation is prohibited under both federal and Massachusetts law. *See* 18 U.S.C. § 1030(a)(2); Mass. Gen. Laws Ann. ch. 266, § 120F.

101. Nor is secret installation of the Contact Tracing App reasonably necessary to carry out any purpose of DPH's enabling act. *See* Mass. Gen. Laws Ann. ch. 17.

102. Accordingly, Defendants' initial and continued installations of the Contact Tracing App onto Android devices without owners' awareness or permission should be declared to be *ultra vires* and enjoined.

Count VI: Common Law Trespass to Chattel

103. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

104. Improper interference with the use and enjoyment of private property is a common law tort in the Commonwealth of Massachusetts. *See Smith v. Wright*, No. 12-ADMS-10032, 2013 WL 1042544 (Mass. App. Ct. 2013).

105. DPH may be enjoined from committing trespassory torts against private property. *See Lane v. Commonwealth*, 401 Mass. 549, 552 (1988) ("We can think of no basis for recognizing some form of governmental immunity that would prevent issuance of an injunction against an ongoing wrong committed systematically and intentionally by a governmental agency for the continuing benefit of the Commonwealth.").

106. Plaintiffs each own one or more personal Android mobile devices.

107. DPH worked with Google to install its Contact Tracing App onto Plaintiffs' personal mobile devices without Plaintiffs' knowledge or permission. The Contact Tracing App causes the mobile device to broadcast via Bluetooth, which rapidly drains the device's batteries.

108. This function interfered with Plaintiffs' use and enjoyment of their private mobile devices by taking up limited storage space and by causing batteries to drain more rapidly. It therefore constitutes trespass to chattel under Massachusetts common law.

109. Accordingly, Defendants' conduct should be declared unlawful, and Defendants should be enjoined from any further trespassory installations of their Contact Tracing App.

Count VII: Violation of the Computer Fraud and Abuse Act

110. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

111. The Computer Fraud and Abuse Act ("CFAA") makes it unlawful to "intentionally access[] a computer without authorization or [to] exceed[] authorized access and thereby … obtain[] information from any protected computer." 18 U.S.C. § 1030(a)(2).

112. A "protected computer" under the CFAA includes any computer "which is used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2). Plaintiffs' Android devices are protected computers used in interstate commerce because they are connected to the internet. *See United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) ("With a connection to the Internet, the … computers were part of a system that is inexorably intertwined with interstate commerce.").

113. DPH's Contact Tracing App is designed to obtain information from Plaintiffs' Android devices, including information regarding personal contacts, movement, and health status.

114. Installing the App on Plaintiffs' Android devices without their knowledge or awareness constitutes unauthorized access.

115. Senior officials in DPH may be enjoined from intentionally committing legal wrongs against private parties. *Lane*, 401 Mass. at 552.

116. Accordingly, Defendants' secret installation of the Contact Tracing App violates the CFAA and should be enjoined. *See* 18 USC § 1030(a)(2), (g).

Count VIII: Unauthorized Access to Computer Systems

117. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

118. Massachusetts law criminalizes unauthorized access to computer systems and states: "Whoever, without authorization, knowingly accesses a computer system by any means, … shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both." Mass. Gen. Laws Ann. ch. 266 § 120F.

119. Installing the App on Plaintiffs' Android devices without their knowledge or awareness constitutes unauthorized access in violation of § 120F.

120. Senior officials in DPH may be enjoined from intentionally committing legal wrongs against private parties. *Lane*, 401 Mass. at 552.

121. Accordingly, Defendants' conduct amounts to a crime under Massachusetts law and should be enjoined.

Count IX: Invasion of Privacy

122. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

123. Massachusetts law provides that "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy." Mass. Gen. Laws Ann. ch. 214, § 1B.

124. A historical record of an individual's past movements and personal associations are private facts of a highly personal or intimate nature.

125. DPH's Contact Tracing App exposes data regarding Android device owners' past movements and personal associations to DPH as well as countless other app developers without the owners' consent.

126. No legitimate interest justifies such disclosure.

127. Senior officials in DPH may be enjoined from intentionally committing legal wrongs against private parties. *Lane*, 401 Mass. at 552.

128. Accordingly, secret installation of the Contact Tracing App is an invasion of privacy under Massachusetts law and should be enjoined.

RELIEF REQUESTED

WHEREFORE, Plaintiffs respectfully request the following relief on behalf of themselves and the class of over one million Android users which they represent:

a. An injunction against continued installation of the DPH's Contact Tracing App on private mobile devices without the knowledge or permission of device owners.

b. An injunction requiring DPH to work with Google to uninstall its Contact Tracing App from private Android mobile devices where the device owner did not give permission for such installation.

c. A declaration that clandestine installations of DPH's Contact Tracing App constitute unreasonable searches in violation of the Fourth Amendment of the U.S. Constitution and Article XIV of the Massachusetts Declaration of Rights.

d. A declaration that clandestine installations of DPH's Contact Tracing App constitute unlawful takings of private property under the Fifth Amendment of the U.S. Constitution and unlawful appropriations under Article X of the Massachusetts Declaration of Rights.

e. A declaration that clandestine installations of DPH's Contact Tracing App are *ultra vires*.

f. A declaration that clandestine installations of DPH's Contact Tracing App constitute unlawful trespasses to chattel under Massachusetts common law.

g. A declaration that clandestine installations of DPH's Contact Tracing App are unlawful and violate federal and Massachusetts computer-crime statutes. *See* 18 U.S.C. § 1030(a)(2); Mass. Gen. Laws Ann. ch. 266, § 120F.

h. A declaration that clandestine installations of DPH's Contact Tracing App constitute unlawful interference with privacy under Massachusetts common law and Mass. Gen. Laws Ann. ch. 214, § 1B.

i. All costs, expenses, and attorney fees allowed under the Equal Access to Justice Act, 5 U.S.C. § 504, 28 U.S.C. § 2412 and/or 42 U.S.C. § 1988(b).

j. Nominal damages of $1.

k. Such other relief as this Court deems just and equitable.

November 14, 2022

Respectfully submitted,

/s/ *Peter Antonelli*
Thomas H. Curran, BBO# 550759
tcurran@curranantonelli.com
Peter Antonelli, BBO# 661526
pantonelli@curranantonelli.com
Curran Antonelli, LLP
Ten Post Office Square, Suite 800 South
Boston, MA 02109
Telephone: (617) 207-8670
Fax: (617) 850-9001

Sheng Li (pro hac vice forthcoming)
Margaret A. Little (pro hac vice forthcoming)
New Civil Liberties Alliance
1225 19th St. NW, Suite 450
Washington, DC 20036
Telephone: 202-869-5210

Attorneys for Plaintiffs